

★NITE P85;W01 2001-077291/09 ★JP 2000324329-A  
Digital content ID providing system, embeds contents ID in the content using electron watermark and sets up digital signature for the ID embedded content

NIPPON TELEGRAPH & TELEPHONE CORP 1999.05.13 1999JP-132112  
W02 (2000.11.24) H04N 1/387, G09C 1/00, 5/00, H04L 9/08

**Novelty:** A directory server (1) authenticates a user when a demand is received from a terminal (2), publishes content ID to the terminal and manages the relationship between the user ID and published contents ID. The contents ID is provided to the digital contents using an electron watermark. The contents ID is embedded to header information and digital signature data of the contents is then setup.

**Use:** For providing ID to digital video contents for copyright protection.

**Advantage:** Even if the discriminative information for contents management is altered, the digital signature data prevents alteration of the contents.

**Description of Drawing(s):** The figure shows the block diagram of the content ID providing system.

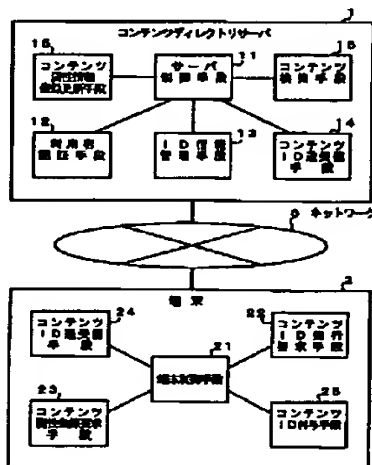
Directory server 1

Terminal 2

(8pp Dwg.No.1/7)

N2001-059172

W01-A05A; W02-J03A2B



A

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-324329

(P2000-324329A)

(43)公開日 平成12年11月24日(2000. 11. 24)

(51)Int.Cl.<sup>7</sup>

識別記号

F I

テマコード(参考)

H 0 4 N 1/387

H 0 4 N 1/387

5 C 0 7 6

G 0 9 C 1/00

G 0 9 C 1/00

6 4 0 A 5 J 1 0 4

5/00

5/00

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 D

審査請求 有 請求項の数4 O L (全 8 頁)

(21)出願番号

特願平11-132112

(22)出願日

平成11年 5月13日(1999. 5. 13)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目 3 番 1 号

(72)発明者 松村 隆宏

東京都新宿区西新宿三丁目19番 2 号 日本

電信電話株式会社内

(72)発明者 田中 清人

東京都新宿区西新宿三丁目19番 2 号 日本

電信電話株式会社内

(74)代理人 100087848

弁理士 小笠原 吉義 (外1名)

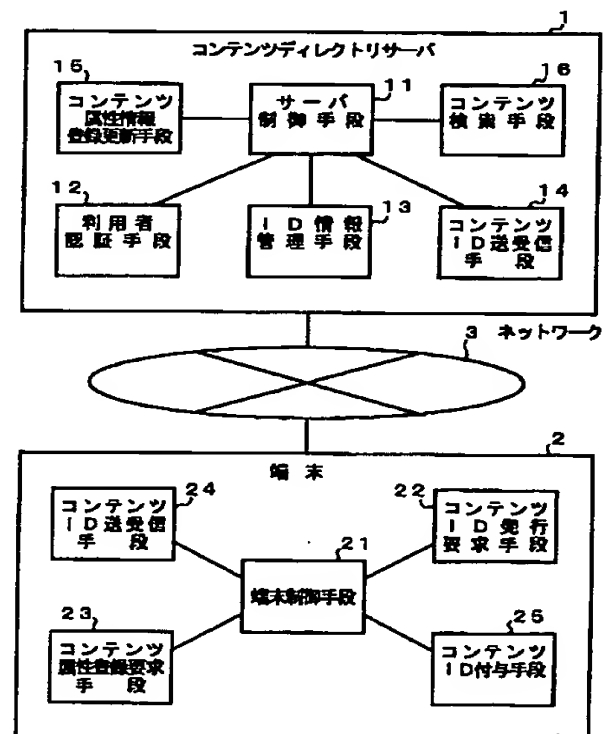
最終頁に続く

(54)【発明の名称】 コンテンツID付与システム

(57)【要約】

【課題】コンテンツ管理用の識別情報が改ざんされても、改ざん防止用のデジタル署名データによって、コンテンツの改ざんを防ぐことができるようにする。

【解決手段】コンテンツディレクトリサーバ1は、端末2からの要求により利用者の認証を行い、コンテンツに対するID情報であるコンテンツIDを発行し、利用者IDと発行したコンテンツIDの関係を管理する。端末2では、コンテンツIDを受信すると、コンテンツID付与手段25によってコンテンツIDをコンテンツに付与する。このとき、コンテンツ本体にはコンテンツIDを電子透かしを用いて埋め込み、ヘッダ情報にはコンテンツIDが埋め込み済みのコンテンツへのデジタル署名データを設定するなどして、コンテンツIDとデジタル署名データを付与する。



## 【特許請求の範囲】

【請求項1】 電子化された情報であるコンテンツまたはその属性情報を管理するためのコンテンツディレクトリサーバと、これにネットワークで接続される端末とで構成されるシステムであって、前記コンテンツディレクトリサーバは、利用者の認証を行う手段と、前記コンテンツに対するID情報であるコンテンツIDを発行し送受信する手段と、利用者IDと発行したコンテンツIDの関係を管理する手段とを備え、前記端末は、前記コンテンツIDの発行を要求する手段と、前記コンテンツIDを送受信する手段と、前記コンテンツIDをコンテンツに付与するコンテンツID付与手段とを備え、前記コンテンツID付与手段は、コンテンツ本体にはコンテンツIDを電子透かしを用いて埋め込み、ヘッダ情報にはコンテンツIDが埋め込み済みのコンテンツへのデジタル署名データを設定するように構成されることを特徴とするコンテンツID付与システム。

【請求項2】 電子化された情報であるコンテンツまたはその属性情報を管理するためのコンテンツディレクトリサーバと、これにネットワークで接続される端末とで構成されるシステムであって、前記コンテンツディレクトリサーバは、利用者の認証を行う手段と、前記コンテンツに対するID情報であるコンテンツIDを発行する手段と、前記コンテンツIDをコンテンツに付与するコンテンツID付与手段と、コンテンツとコンテンツIDを前記端末に送信する手段と、利用者IDと発行したコンテンツIDの関係を管理する手段とを備え、前記端末は、前記コンテンツIDの発行を要求する手段と、コンテンツを送受信する手段とを備え、前記コンテンツID付与手段は、コンテンツ本体にはコンテンツIDを電子透かしを用いて埋め込み、ヘッダ情報にはコンテンツIDが埋め込み済みのコンテンツへのデジタル署名データを設定するように構成されることを特徴とするコンテンツID付与システム。

【請求項3】 電子化された情報であるコンテンツまたはその属性情報を管理するためのコンテンツディレクトリサーバと、これにネットワークで接続される端末とで構成されるシステムであって、前記コンテンツディレクトリサーバは、利用者の認証を行う手段と、前記コンテンツに対するID情報であるコンテンツIDを発行し送受信する手段と、利用者IDと発行したコンテンツIDの関係を管理する手段とを備え、前記端末は、前記コンテンツIDの発行を要求する手段と、前記コンテンツIDを送受信する手段と、前記コンテンツIDをコンテンツに付与するコンテンツID付与手段とを備え、前記コンテンツID付与手段は、ヘッダ情報にコンテンツID、およびコンテンツへのデジタル署名データを設定するように構成されることを特徴とするコンテンツID付与システム。

【請求項4】 電子化された情報であるコンテンツまた

はその属性情報を管理するためのコンテンツディレクトリサーバと、これにネットワークで接続される端末とで構成されるシステムであって、前記コンテンツディレクトリサーバは、利用者の認証を行う手段と、前記コンテンツに対するID情報であるコンテンツIDを発行する手段と、前記コンテンツIDをコンテンツに付与するコンテンツID付与手段と、コンテンツとコンテンツIDを前記端末に送信する手段と、利用者IDと発行したコンテンツIDの関係を管理する手段とを備え、前記端末は、前記コンテンツIDの発行を要求する手段と、コンテンツを送受信する手段とを備え、前記コンテンツID付与手段は、ヘッダ情報にコンテンツID、およびコンテンツへのデジタル署名データを設定するように構成されることを特徴とするコンテンツID付与システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、デジタルコンテンツまたはその著作権等の属性情報の登録更新等の管理を行うシステムに関する。

## 【0002】

【従来の技術】近年、デジタルコンテンツ流通の時代が始まりつつある。しかし、デジタルコンテンツは保存・複写・加工・転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルコンテンツの著作権処理には的確な方法がなく、著作権法あるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【0003】このような状況において、データベース化されたデジタルコンテンツの著作権をどのように扱うかが大きな問題となるが、これまでのところ、そのための著作権管理手段で完成されたものはない。

【0004】これに関連する従来技術としては、例えば特開平11-7241号公報「電子透かしを利用するデジタルコンテンツ管理システム」、特開平10-302008号公報「データコンテンツ流通システム」、特開平10-254909号公報「データ管理システム」等で開示された技術がある。

【0005】例えば、特開平11-7241号の電子透かしを利用するデジタルコンテンツ管理システムでは、デジタルコンテンツ管理プログラムをマイクロカーネルとしてユーザ装置のオペレーティングシステムに組み込み、ネットワークあるいはデータ放送を利用して、デジタルコンテンツ管理プログラムとリンクする監視プログラムまたは監視コマンドをユーザ装置に送信し、デジタルコンテンツの不正利用を監視する。不正利用されたデジタルコンテンツには、可視透かしを埋め込み、以後の利用を抑制する。正規の利用であっても不可視の透かしを埋め込むことにより、複写・転送等の経路を確認する

ことを可能にする。また、公開鍵を公開鍵配布画面に記入してネットワークあるいは放送により配布する。公開鍵配布画面には、公開鍵所有者あるいは利用者の情報が不可視電子透かしとして埋め込まれたイメージ情報を添付し、この電子透かしにより公開鍵あるいは利用者の正当性を確認する。

【0006】また、特開平10-302008号公報のデータコンテンツ流通システムでは、データのコンテンツとしてオブジェクトを取り扱い、データコンテンツの加工はオブジェクトであるデータコンテンツを加工プログラムによって加工することによって行う。加工データコンテンツは、原データコンテンツと加工プログラムによる加工内容を記載した加工シナリオとによって表現する。流通するのは、暗号化された加工シナリオのみであり、暗号化加工シナリオを入手したユーザは、鍵管理センタから入手した暗号鍵を用いて暗号化加工シナリオを復号し、加工シナリオに従ってデータベースから原データコンテンツを入手し、加工データコンテンツを再構成する。加工シナリオの販売を希望する者がいる場合には、競売を行い、加工シナリオの使用権を販売する。

【0007】また、特開平10-254909号公報のデータ管理システムでは、データコンテンツの盗用や漏洩の防止のため、データ管理センタで、ユーザに供給するデータコンテンツにユーザデータを電子透かしとして埋め込み、データコンテンツを暗号鍵で暗号化して供給する。暗号化データコンテンツは、データ管理センタからの暗号鍵を用いて復号して利用され、保存では別の暗号鍵を用いて暗号化される。データコンテンツを他のユーザに複写・転送するには、他のユーザのユーザデータを電子透かしとして埋め込むためのシナリオをデータ管理センタに登録し、電子透かしを埋め込んだデータコンテンツを別の暗号鍵で暗号化して供給する。シナリオで他のユーザの正当性が確認されると、他のユーザに別の暗号鍵を配送し、暗号化データコンテンツをその別の暗号鍵で復号して利用させ、保存では別の暗号鍵で暗号化する。データコンテンツの不正な複写・転送が行われた場合には、電子透かしの確認でその利用者を特定することができる。

【0008】

【発明が解決しようとする課題】しかしながら、以上のような従来技術では、コンテンツ管理用の識別情報（コンテンツID）を登録の正当性を確保して発行すると同時に、コンテンツ管理用の識別情報またはコンテンツの属性情報をもとに映像または音楽等のコンテンツに関してユーザにコンテンツの検索を可能にするにあたって、電子透かしを利用してコンテンツIDを付与する場合、コンテンツIDの改ざんの問題があった。ここでいう改ざんの問題とは、既に付与済みのコンテンツに対して故意にコンテンツIDを再び埋め込むことなどにより、コンテンツIDを書き換える行為などをいう。本発明は、

コンテンツに付与するコンテンツIDの改ざんの防止を課題とする。

【0009】

【課題を解決するための手段】本発明は、コンテンツに対するID情報であるコンテンツIDの発行を要求する手段、コンテンツIDを送受信する手段、およびコンテンツIDをコンテンツに付与する手段を有する端末と、利用者の認証を行う手段、コンテンツIDを発行し送受信する手段、および利用者IDと発行したコンテンツIDの関係を管理する手段を有するコンテンツディレクトリサーバとで構成されるコンテンツID付与システムであって、コンテンツID付与手段が、コンテンツ本体にはコンテンツIDを電子透かしを用いて埋め込み、ヘッダ情報にはコンテンツIDが埋め込み済みのコンテンツへのデジタル署名データを設定するように構成されることを特徴とする。

【0010】または、コンテンツIDの発行を要求する手段、およびコンテンツを送受信する手段を有する端末と、利用者の認証を行う手段、コンテンツIDを発行しコンテンツIDをコンテンツに付与する手段、コンテンツとコンテンツIDを端末に送信する手段、および利用者IDと発行したコンテンツIDの関係を管理する手段を有するコンテンツディレクトリサーバとで構成されるコンテンツID付与システムであって、コンテンツID付与手段が、コンテンツ本体にはコンテンツIDを電子透かしを用いて埋め込み、ヘッダ情報にはコンテンツIDが埋め込み済みのコンテンツへのデジタル署名データを設定するように構成されることを特徴とする。

【0011】ここで、前者と後者は、構成において、コンテンツIDを付与する手段が端末にあるかサーバにあるかが異なる。そして、コンテンツIDを付与する手段を各々さらに以下のように構成してもよい。

【0012】すなわち、コンテンツID付与手段が、コンテンツのヘッダ情報に、コンテンツIDとコンテンツへのデジタル署名データとを設定するように構成してもよい。

【0013】ここで、デジタル署名データはコンテンツID情報の改ざんを防止するための情報である。なお、デジタル署名に関しては、「現代暗号理論（池野信一、小山謙二著、1986年電子情報通信学会発行）」の217ページ～239ページ、特に235ページ～236ページに、詳細な技術の内容が開示されている。

【0014】

【発明の実施の形態】図1は、コンテンツID付与システムのブロック構成図である。図1に示すように、コンテンツディレクトリサーバ1と利用者の端末2とは、ネットワーク3で接続される。

【0015】コンテンツディレクトリサーバ1のサーバ制御手段11が、利用者認証手段12と、ID情報管理手段13と、コンテンツID送受信手段14と、コンテ

ンツ属性情報登録更新手段15と、コンテンツ検索手段16との同期を制御する。

【0016】利用者認証手段12は、端末2からのコンテンツID発行要求を受けて、要求者の認証を行う手段である。認証の方法としては、どのような方法を用いてもよいが、例えば公開鍵と秘密鍵を用いる公開鍵暗号方式を使ってもよい。特開平10-39752号公報「公開鍵暗号による通信および認証方法、ならびにそれらの装置」に記述された手順を用いると、強度の高い暗号化を実現することができる。

【0017】この特開平10-39752号公報に記載されている公開鍵暗号方式では、従来の有理整数環上の公開鍵暗号と比較して、完全解読に対しては同程度以上の強度を持ち、同報通信攻撃に対して従来より高い強度を持つ暗号化を実現するため、鍵生成装置は、代数体上の整数環 $O$ における素イデアル $(p)$ 、 $(q)$ を生成して第1の秘密鍵とし、その積 $(n) = (p)(q)$ の剰余類を第1の公開鍵とする。また、 $(p)$ 、 $(q)$ から第2の秘密鍵 $d$ と第2の公開鍵 $e$ を生成する。暗号化装置は、入力された平文 $M$ をブロックに分割し、イデアル $(n)$ を法とする $e$ 乗演算により暗号化を行い、暗号文 $(C_0, C_1, \dots, C_{r-1})$ を通信路に出力する。復号化装置は、入力された暗号文のブロックに対しイデアル $(n)$ を法とする $d$ 乗演算により復号化を行い、復号化された平文ブロックを統合して、平文 $M$ を出力する。他にも種々の公開鍵暗号方式があり、これらの具体的手順についてはよく知られている技術であるので、ここでの詳細な説明は省略する。

【0018】コンテンツID送受信手段14は、利用者認証手段12による利用者認証を受けてコンテンツIDを発行するとともに、コンテンツID情報を端末2との間で送受信する手段である。ID情報管理手段13は、認証した利用者に対して発行したコンテンツID情報を、その利用者に関係付けてデータベースで管理する手段である。コンテンツ属性情報登録更新手段15は、端末2から受信したコンテンツID別のコンテンツ属性情報をもとに、コンテンツID毎のコンテンツ属性情報をデータベースに登録更新して管理する手段である。

【0019】コンテンツ検索手段16は、コンテンツID毎の属性情報を通知したり、コンテンツ属性情報の検索条件を絞り込んだときに検索条件に合致するコンテンツの集合を通知する手段である。

【0020】また、図1に示す端末2において、端末制御手段21は、コンテンツID発行要求手段22と、コンテンツ属性登録要求手段23と、コンテンツID送受信手段24と、コンテンツID付与手段25との同期を制御する。

【0021】コンテンツID発行要求手段22は、コンテンツディレクトリサーバ1に対してコンテンツIDの発行を要求する手段である。コンテンツID送受信手段

24は、コンテンツディレクトリサーバ1で発行されたコンテンツIDを受け取るとともに、コンテンツIDをコンテンツディレクトリサーバ1に送信する手段である。

【0022】コンテンツID付与手段25は、コンテンツディレクトリサーバ1が発行したコンテンツIDをコンテンツに付与する手段である。付与の方法として、電子透かしによりコンテンツ本体に埋め込むとか、またはファイルのヘッダ情報にコンテンツIDを設定するとかの方法を用いることができる。電子透かしの具体的手順については、例えば特開平10-191025号公報「デジタル画像への情報埋め込み装置」、特開平10-145757号公報「電子透かしの挿入方法及び抽出方法」等に記述された手順を用いてもよい。

【0023】特開平10-191025号公報に記載されている装置では、画像データの円滑な流通を促進させることなどのために、画像データへの情報の追加埋め込みを、安全・確実に行うことができるようにすることを目的として、符号化した画像データを元の画像に復元する逆符号化装置の処理と、画像データに情報を埋め込む電子透かし挿入装置の処理とを分離不可能に構成し、画像データから元の画像を復元する際に、逆符号化装置によって復元処理を行うとともに、電子透かし挿入装置によって情報の埋め込みを行うことにより、逆符号化装置にて元の画像を得る段階で情報を埋め込む。

【0024】また、特開平10-145757号公報に記載されている方法では、部分画像に透かし情報を蓄積し、その部分画像から透かし情報を抽出することによって信頼性を改善することを目的として、以下の手順で処理を行う。まず、透かし処理されるデータを複数の小区域に分割する。透かし処理されるデータの周波数係数をそれぞれの小区域で算出する。透かし信号を擬似乱数ノイズシーケンスにマッピングすることによって、挿入される透かし信号を拡散スペクトルに変調する。平均出力の関数としてのPNをデータのそれぞれの周波数係数にスペクトル形成する。そして、スペクトル形成されたそれぞれのPNシーケンスをそれぞれの小区域のデータの所定係数に挿入する。こうして画像、映像、及び音声データを含むデータの電子透かし処理を、透かしをデータの小区域あるいは部分画像に繰り返し挿入することによって行う。同様に透かしをデータの小区域から繰り返し抽出する。

【0025】コンテンツ属性登録要求手段23は、発行されたコンテンツIDに関するコンテンツの属性情報をコンテンツディレクトリサーバ1に対して登録または更新するように要求する手段である。なお、利用者認証手段を端末2にも付け加えてもよい。

【0026】図2は、利用者ID情報、コンテンツID情報、コンテンツ属性情報の各データ構造の例を示すものである。利用者ID情報は、利用者が暗号通信の認証

機関等から与えられた識別用情報（利用者番号）である。コンテンツID情報は、コンテンツの識別のためにコンテンツディレクトリサーバが利用者に対して与える識別用情報である。図2（B）に示す例では、利用者IDと作品番号（作品ID）のペアの情報で構成されている。コンテンツ属性情報は、コンテンツID毎にそのコンテンツの属性情報を格納するものであり、例えば登録年月日、メディア種別（静止画像、動画像、音楽等）、検索用分類コード1・2・3、コンテンツ格納アドレスで構成される。ここでコンテンツ格納アドレスには、コンテンツの閲覧などが可能なように掲載されているホームページのアドレス、またはそのコンテンツを購入するための連絡先の通信アドレス等が含まれる。

【0027】図3は、コンテンツ改ざん防止用デジタル署名データの付与方法の例を示すものである。図3

（A）に示すパターンP1は、コンテンツIDをコンテンツ本体に電子透かしで埋め込み、コンテンツの改ざん防止用のデジタル署名データをヘッダ情報の中に設定するものである。図3（B）に示すパターンP2は、コンテンツIDと、コンテンツの改ざん防止用のデジタル署名データをヘッダ情報の中に設定するものである。

【0028】次に本実施の形態での動作例を、コンテンツID登録手順、コンテンツ属性登録手順、コンテンツ検索手順で説明する。この動作例は、コンテンツIDのコンテンツへの付与を端末で行う場合の動作例であるが、サーバ側でコンテンツIDの付与を行う場合も同様である。

【0029】図4は、コンテンツID登録手順の例を示す。端末2のコンテンツID発行要求手段22からコンテンツIDの発行要求が起こり（ステップS10）、それを受けて発行要求した利用者の認証を、利用者ID情報をもとに利用者認証手段12が行い（S11）、利用者が正しく認証されれば、コンテンツID送受信手段14がコンテンツIDを発行し（S12）、端末2に送信する（S13）。さらに、ID情報管理手段13が、利用者IDと発行したコンテンツIDの組の対応関係をデータベースに保存する（S14）。

【0030】端末2では、コンテンツID送受信手段24がコンテンツIDを受け取り（S15）、コンテンツID付与手段25がコンテンツIDをコンテンツに付与する（S16）。このとき、コンテンツID付与手段25は、コンテンツIDの付与だけでなく、コンテンツIDの改ざん防止のためのデジタル署名データの付与を行う。図3で説明した2つのパターンP1、P2により、コンテンツIDとデジタル署名データを付与する。コンテンツID付与が完了すると、端末2は完了通知をコンテンツディレクトリサーバ1に送る。なお、コンテンツIDの電子透かしによる埋め込みに関しては、固定鍵を用いて電子透かしを埋め込み、コンテンツID付与の前に、既にコンテンツIDが付与されているか否かを電子

透かしを固定鍵により読み出すことにより調べ、もし既に埋め込まれていれば、付与を行わないように構成してもよい。

【0031】図5は、コンテンツ属性登録手順の例を示す。端末2のコンテンツ属性登録要求手段23が、コンテンツ属性情報の登録・更新を要求すると（S20）、コンテンツディレクトリサーバ1の利用者認証手段12が利用者を認証し（S21）、正しく認証されたら、端末2からコンテンツIDとそのコンテンツIDに関する属性情報をコンテンツディレクトリサーバ1に送り（S22）、コンテンツディレクトリサーバ1がこれを受け取ると（S23）、コンテンツIDと利用者IDの組み合わせを、ID情報管理手段13で管理している内容と比較して管理内容と合致していることを確認する（S24）。確認が済めば、コンテンツ属性情報登録更新手段15がそのコンテンツIDに関するコンテンツ属性情報を登録または更新する（S25）。

【0032】図6は、コンテンツ検索手順の例を示す。コンテンツディレクトリサーバ1のコンテンツID送受信手段14がコンテンツIDを端末2から受信すると（S30）、そのコンテンツ属性情報を端末2に送信する（S31）。さらに、端末2からコンテンツ属性情報の属性パラメータを指定した検索要求があれば（S32）、指定条件に一致するコンテンツをコンテンツディレクトリサーバ1のコンテンツ検索手段16が検索し（S33）、検索結果を端末2に送信する（S34）。

【0033】図1に示す例では、電子透かしを用いてコンテンツにコンテンツIDを付与する処理を、端末2側でコンテンツID付与手段25が行っているが、このコンテンツIDの付与を、サーバ側で行うように構成することもできる。

【0034】図7は、その本発明の第2の実施の形態を示すブロック構成図である。図7において、図1と同符号のものは図1に示すものと同様の機能を持つ。端末2'は、コンテンツディレクトリサーバ1'に対してコンテンツIDの発行を要求する際に、そのコンテンツをコンテンツディレクトリサーバ1'に送信する。

【0035】コンテンツディレクトリサーバ1'では、コンテンツ・コンテンツID送受信手段17により、コンテンツIDの発行要求とコンテンツとを受けて、発行要求した利用者の認証を、利用者認証手段12が利用者ID情報をもとに行う。利用者が正しく認証されれば、コンテンツIDを発行し、コンテンツID付与手段18によって、受け取ったコンテンツにコンテンツIDを付与する。このとき、コンテンツID付与手段18は、コンテンツIDの付与だけでなく、コンテンツIDの改ざん防止のためのデジタル署名データの付与を、図3で説明した2つのパターンにより行う。そのコンテンツとコンテンツIDとをコンテンツ・コンテンツID送受信手段17によって端末2'に送信する。

【0036】端末2'では、コンテンツ・コンテンツID送受信手段26によって、コンテンツディレクトリサーバ1'から送信されたコンテンツとコンテンツIDを受け取る。なお、他の部分の処理機能については、前述した図1のものと同様であるので、ここでの説明は省略する。

【0037】

【発明の効果】本発明によれば、コンテンツIDが改ざんされても、改ざん防止用のデジタル署名データがあるため、コンテンツの改ざんを防ぐ効果がある。

【0038】ここで、例えば図3(A)に示すようなパターンP1では、コンテンツの改ざんの有無を、ヘッダ情報のデジタル署名データをもとにして判定することができる。同様に、図3(B)に示すパターンP2でも、改ざんの有無を判定することができる。

【図面の簡単な説明】

【図1】コンテンツID付与システムのブロック構成図である。

【図2】利用者ID情報、コンテンツID情報、コンテンツ属性情報の各データ構造の例を示す図である。

【図3】コンテンツIDとコンテンツ改ざん防止用デジ

タル署名データの付与方法の例を示す図である。

【図4】コンテンツID登録手順の例を示す図である。

【図5】コンテンツ属性登録手順の例を示す図である。

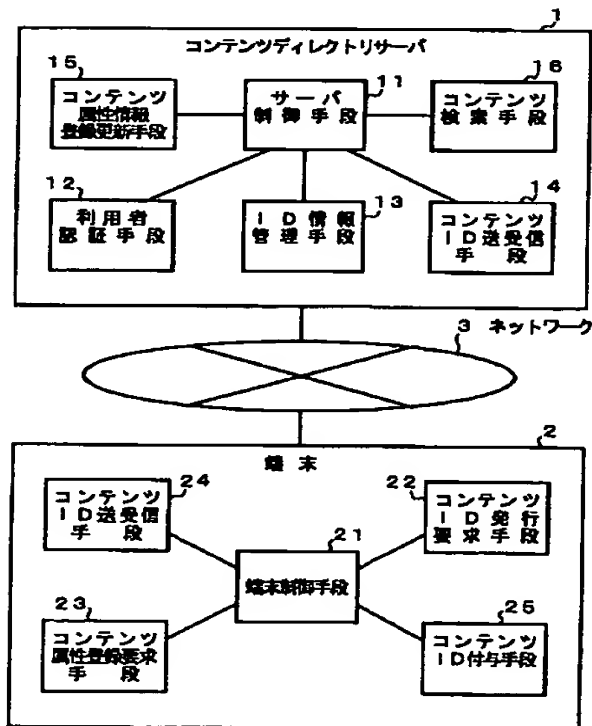
【図6】コンテンツ検索手順の例を示す図である。

【図7】他のコンテンツID付与システムのブロック構成図である。

【符号の説明】

- 1 コンテンツディレクトリサーバ
- 11 サーバ制御手段
- 12 利用者認証手段
- 13 ID情報管理手段
- 14 コンテンツID送受信手段
- 15 コンテンツ属性情報登録更新手段
- 16 コンテンツ検索手段
- 2 端末
- 21 端末制御手段
- 22 コンテンツID発行要求手段
- 23 コンテンツ属性登録要求手段
- 24 コンテンツID送受信手段
- 25 コンテンツID付与手段
- 3 ネットワーク

【図1】



【図2】

データ構造

(A) 利用者ID情報

利用者番号
-------

(B) コンテンツID情報

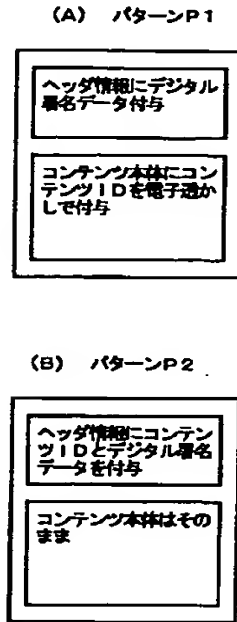
利用者ID	作品番号
-------	------

(C) コンテンツ属性情報

登録年月日	メディア種別
検索用分類コード1	検索用分類コード2
検索用分類コード3	コンテンツ格納アドレス

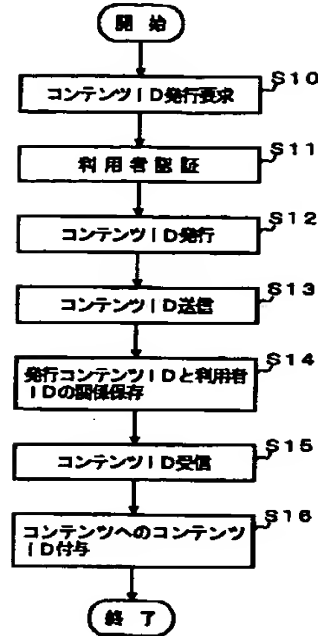
【図3】

コンテンツIDとコンテンツ取らん防止用デジタル署名データの付与方法



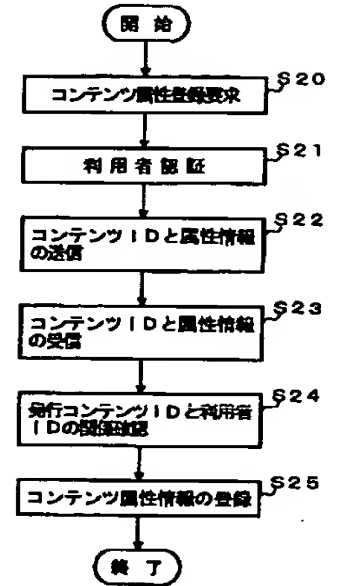
【図4】

コンテンツID登録手順



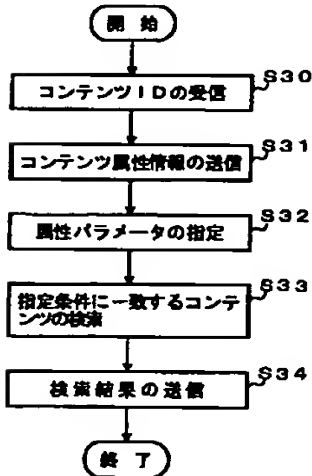
【図5】

コンテンツ属性登録手順

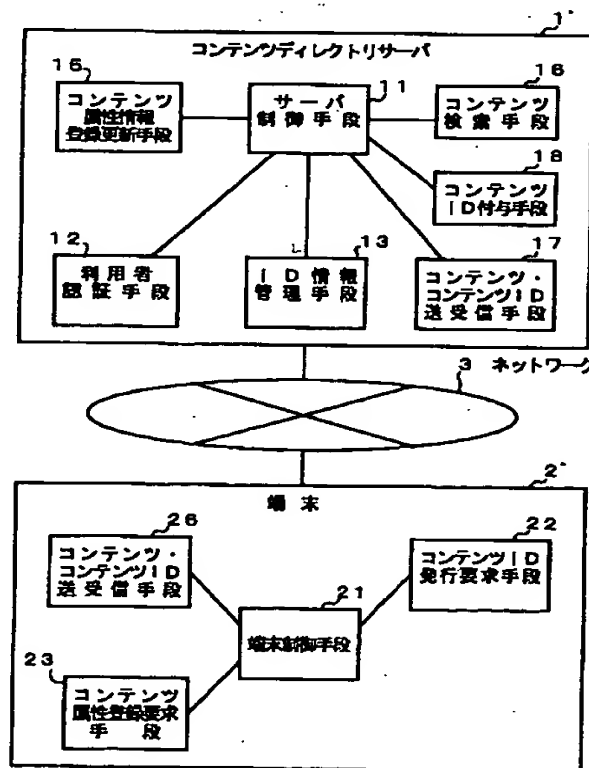


【図6】

コンテンツ検索手順



【図7】





フロントページの続き

(72)発明者 堀岡 力  
東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72)発明者 山中 喜義  
東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

Fターム(参考) 5C076 AA14 BA06

5J104 AA07 AA09 AA14 AA16 EA10

KA01 NA36 PA07 PA14